

## **REMARKS**

Applicant hereby responds to the Office Action dated February 24, 2004 within the shortened three month statutory period for response. The Examiner rejects claims 1-19. Upon entry of the foregoing amendments, Applicant adds new claims 20-23, so claims 1- 23 remain pending in the application. Support for the various amendments may be found in the originally filed specification, claims, and figures. No new matter has been introduced by these amendments. Reconsideration of this application is respectfully requested.

The Examiner rejects claims 1, 3, 8-9, 14 and 16 under 35 USC 102(a) as being anticipated by Atkinson (5,892,904). Applicant respectfully traverses these rejections. Atkinson is limited to certifying executable code, such as an .EXE, .OCX, or a Java Class file. The purpose of Atkinson is to help safeguard against downloading malicious code by certifying the publisher's identification through a third party certifying organization. In Atkinson, the publisher of the code component (.ocx, .exe, Java class file, etc.) applies for a digital certificate with a certifying agency by providing information such as name, organization, address, phone number, and etc. The publisher attaches his/her digital certificate to the code file by entering a registration number provided to the publisher from the certifying agency. At the time that the digital certificate is attached to the code component, hash data is attached to the certificate. The hash data is similar to a fingerprint of the code component, along with other data such as a date and time stamp. If the code is later modified in any way, the digital certificate is rendered invalid. A public key assigned to the publisher is also attached to the code, thereby associating the code with the certification agency's public key. When a user attempts to download a code component over the Internet, logic within the browser application checks for the presence of a digital certificate. The digital certificate is decrypted with the certification agency's public key. The digital certificate is then decoded with the publisher's public key allowing validation of the certificate by comparing the current hash data to the decoded certificate. As such, Atkinson attempts to confirm that the contents of the executable code has not changed.

In contrast, the presently claimed invention is directed toward authenticating the source of web pages and not certifying that the executable code is unchanged. A webpage includes format data and possibly links to executable code, but the presently claimed invention authenticates the web page and does not certify that the code found in the link is unchanged. The present invention helps to safeguard users from entering private information into web pages that

have been misrepresented. For example, an identity thief could copy entire web pages from a legitimate company, such as Amazon.com. The thief may then, by purchasing a domain name that is only slightly different than that of the legitimate company (e.g., Anazon.com), the identity thief may pose the copied pages on the unauthorized website. The identity thief could potentially steal information from those who stumble upon the unauthorized domain.

As such, Atkinson is directed toward protecting a computer user from downloading malicious executable code, while the presently claimed invention is directed toward ensuring that requested web page source is authentic. While the presently claimed invention and Atkinson may generally disclose an authentication key (or public key), the use of the authentication key is very different and for a very different purpose. Particularly, the presently claimed invention uses an authentication key to verify the authenticity of the source of the web page. However, Atkinson does not use an authenticity key to verify the source of the code component. Rather, Atkinson uses the authentication key to decode the certificate in order to validate the hash data. As such, the Atkinson validation is based on the hash data for the code to determine if the code has been modified in any way. In contrast, the presently claimed invention does not test to authenticate if web page content is unchanged; rather, the presently claimed invention verifies that the page source is authentic. Moreover, in Atkinson, the certificate is generated once in advance to publishing the code component, while one embodiment of the presently claimed invention utilizes an authentication server to dynamically sign web page content. As such, Atkinson does not include, for example, "authenticating the authenticity key to verify the source of the formatted data", as required in independent claims 1 and 14.

More particularly, while Atkinson and the present invention may employ the concept of private/public keys, they do so quite differently. Atkinson uses the public key of the certifying agency to decipher the public key of the publisher. The decrypted public key of the publisher is then used to decode the certificate which is attached to the executable. In contrast, the presently claimed invention uses a browser plug-in to compare the public key inserted by the authentication server with a public key existing in the browser plug-in. As such, Atkinson also does not include "a browser plug-in interfacing with a MIME type to authenticate the formatted data private key", as required in dependent claim 21.

With respect to independent claims 8 and 13, Applicant respectfully asserts that Atkinson does not specifically disclose, teach or suggest an "authentication server". Moreover, Atkinson

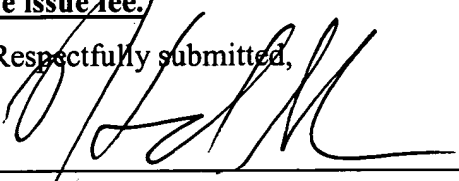
does not disclose, teach or suggest a server "being configured to insert an authenticity key into the web page requested from said client thereby facilitating said client to authenticate the authenticity key to verify the source of the web page", as similarly required in independent claims 8 and 13.

The Examiner next rejects claims 2, 4, 6, 10-11, 13, 15 and 17 under 35 USC 103(a) as being unpatentable over Atkinson (5,892,904) in view of Wallent (6,366,912). Applicant respectfully traverses these rejections. Applicant asserts that claims 2, 4, 6, 10-11, 13, 15 and 17 are patentable for the same reasons as set forth above for differentiating the respective independent claims from the prior art and from Atkinson.

The Examiner next rejects claims 5, 7, 12 and 18-19 under 35 USC 103(a) as being unpatentable over Atkinson (5,892,904) and Wallent (6,366,912) and further in view of Houser (5,606,609). Applicant respectfully traverses these rejections. Applicant asserts that claims 5, 7, 12 and 18-19 are patentable for the same reasons as set forth above for differentiating the respective independent claims from the prior art and from Atkinson.

In view of the above remarks and amendments, Applicant respectfully submits that all pending claims properly set forth that which Applicant regards as its invention and are allowable over the cited prior art. Accordingly, Applicant respectfully requests allowance of the pending claims. The Examiner is invited to telephone the undersigned at the Examiner's convenience, if that would help further prosecution of the subject Application. Applicant authorizes and respectfully requests that any fees due be charged to Deposit Account No. 19-2814. **This statement does NOT authorize charge of the issue fee.**

Respectfully submitted,

  
Howard Sobelman  
Reg. No. 39,038

Dated: March 25, 2004

**SNELL & WILMER L.L.P.**  
400 E. Van Buren  
One Arizona Center  
Phoenix, Arizona 85004  
Phone: 602-382-6228  
Fax: 602-382-6070  
Email: [hsobelman@swlaw.com](mailto:hsobelman@swlaw.com)